

Hermes Agent connector changelog

Use this page to decide whether a Hermes Agent connector change requires a new artifact, admission record, provider qualification, migration, or caller update. It records only changes established from the reviewed source range.

SECTION	Connectors
TYPE	Connector
PROTOCOL	AIP 1.0
SOURCE	docs/connectors/hermes-agent/changelog.md

Release status: the reviewed snapshot is not a tagged release. The reviewed repository tags `034a5206` as `v1.0.0`; the documentation revision is five commits later and still declares workspace version `1.0.0`. Use the full source and artifact identities to distinguish these states.

Identify the exact version

Identity	Published baseline	Reviewed source snapshot
Source commit	<code>034a520608eea44e6b14e61c34734bd402d989c0</code>	<code>97be86e9efedf07ecf1783b03800f683f107fb04</code>
Source position	Tagged	Five commits after the tag
Publication status	Published tag in the reviewed repository	Unreleased source in the reviewed ancestry
Workspace version	<code>1.0.0</code>	<code>1.0.0</code>
Native AIP version	<code>1.0</code>	<code>1.0</code>
Hermes capabilities per endpoint	27	35
Hermes upstream source pin	Not declared in connector compatibility metadata	<code>7426c09beee73bdff94d916015bac71384f6bc92</code>
Standalone Hermes host	Absent	<code>aip-host-hermes-agent</code>

An operator record for the reviewed snapshot needs the full source commit, tree state, immutable host image, manifest digest, connector version ID, release ID, and Hermes artifact. A tag or `1.0.0` image label cannot replace that tuple.

Reviewed source snapshot

The entries below describe Hermes-relevant differences between `v1.0.0` and `97be86e9`. They are source changes, not proof that an artifact was built, published, deployed, or qualified.

Added

- A dedicated `aip-host-hermes-agent` binary and common standalone-host image path.
- Registry admission, tenant-scoped routing, replica leases, health, drain,

and recovery integration in the connector-fleet topology.

- An exact Hermes upstream revision in manifest compatibility metadata.
- Eight endpoint-qualified scheduled-job operations.
- Product-image and controlled-fleet qualification procedures for the Hermes

host.

- Job-route tests for path IDs, list queries, body partitioning, capability classification, approval, risk, and idempotency metadata.

The added operations are:

Operation	Provider route	Risk and control
<code>jobs_list</code>	GET <code>/api/jobs</code>	Low-risk read
<code>job_create</code>	POST <code>/api/jobs</code>	Medium risk; approval and idempotency required
<code>job_get</code>	GET <code>/api/jobs/{job_id}</code>	Low-risk read
<code>job_update</code>	PATCH <code>/api/jobs/{job_id}</code>	Medium risk; approval and idempotency required
<code>job_delete</code>	DELETE <code>/api/jobs/{job_id}</code>	High risk; approval and idempotency required
<code>job_pause</code>	POST <code>/api/jobs/{job_id}/pause</code>	Medium risk; approval and idempotency required
<code>job_resume</code>	POST <code>/api/jobs/{job_id}/resume</code>	Medium risk; approval and idempotency required
<code>job_run</code>	POST <code>/api/jobs/{job_id}/run</code>	High-risk agent action; approval and idempotency required

Job identifiers are exactly 12 lowercase hexadecimal characters. The connector places the identifier in the path and does not forward `job_id` or the AIP idempotency key in an update body.

Changed

Seven existing session-management operations change from `CapabilityKind::Resource` to `CapabilityKind::Tool`:

- `sessions_list`;
- `session_create`;
- `session_get`;
- `session_patch`;
- `session_delete`;
- `session_messages`;
- `session_fork`.

Their capability IDs and provider routes do not change in this source range. The classification change makes every published Hermes API operation action-routable. The current manifest test rejects any remaining `CapabilityKind::Resource` entry.

The production delegated-result resolver also gains a constructor that accepts only the Action queue and lifecycle store. The standalone host uses that constructor instead of receiving the complete central runtime.

Security and isolation boundary

The standalone host makes these ownership rules deployable:

- every endpoint descriptor must match the host tenant;

- endpoint credentials are read from bounded owner-controlled files;
- an omitted operator-policy file leaves first-class delegation disabled;
- the host installs durable approval, profile-state, Action, and lifecycle

stores from its own runtime database;

- registry identity, artifact digest, manifest, credential revision, and

endpoint set are fixed outside Action input.

These controls describe the reviewed standalone topology. They do not qualify an arbitrary deployment or change the trust requirements of native AIP.

Deprecated, removed, or renamed

No Hermes capability ID from the 27-operation `v1.0.0` baseline is removed or renamed in the reviewed range. The source defines no connector-specific deprecation or removal date.

The session kind correction can still affect callers that cached capability metadata or projected `Resource` entries differently. Treat it as a contract metadata migration even though the capability IDs remain stable.

Apply the required migration

Change encountered	Required action	Do not do
Bundled connector to standalone host	Follow the bounded bundled-to-fleet migration; preserve endpoint, tenant, credential, Action, approval, provider-handle, operator-binding, and stream evidence	Run both mutation paths without an explicit fence
New snapshot with the same <code>1.0.0</code> version	Admit a new immutable connector version with exact source, image, manifest, and release identities	Replace an existing version record or identify it only as <code>1.0.0</code>
Catalogue expands from 27 to 35	Refresh tenant discovery, allowlists, generated clients, and expected catalogue digests	Assume an exact-count check is a provider failure
Session kind changes to <code>Too1</code>	Rediscover the stable capability IDs through the native Action or MCP tool path	Continue treating session operations as <code>ResourceList</code> or <code>ResourceRead</code> entries
Scheduled jobs are adopted	Add reviewed approval, idempotency, delivery, scheduler-state, and cleanup policy for each mutation	Treat a successful submission as proof of one execution
Hermes source or image changes	Re-audit the route and event matrix, update the upstream identity, and requalify affected paths	Keep the old compatibility pin while promoting new provider bytes

Stabilize the standalone topology before adopting the added job family. A process migration, capability expansion, and provider upgrade need separate evidence and rollback decisions.

Retain the compatibility pins

The reviewed snapshot selects these values in source:

Surface	Pin
Connector ID	<code>hermes-agent</code>
Connector profile	<code>aip.connector.hermes_agent.v1</code>
Manifest format	<code>aip-manifest/v1</code>
Workspace and host version	<code>1.0.0</code>
Native AIP version	<code>1.0</code>
Hermes upstream commit	<code>7426c09beee73bdf94d916015bac71384f6bc92</code>
Capability shape	<code>cap:hermes_agent:<endpoint_id>:<operation></code>

Surface	Pin
Capabilities per endpoint	35
Standalone host	<code>aip-host-hermes-agent</code>
Effective endpoint ceiling	14 under the fixed 512-capability manifest limit
Standalone version-ID shape	<code>cver_hermes_agent_1_0_0_<release-id></code>

The upstream commit identifies reviewed source, not a built Hermes image or model route. Changing either deployment without changing connector source does not establish compatibility with the new artifact.

Decide when a new connector version is required

Create and admit a new immutable connector version when a change affects any of these properties:

- capability IDs, kinds, schemas, risk, approval, retry, streaming, or idempotency semantics;
- provider method, path, query, request body, response, or SSE event mapping;
- endpoint normalization, tenant binding, credential scope, redirect policy, or secret resolution;
- operator binding, delegated identity, approval generation, cancellation, or result integrity;
- artifact bytes, dependencies, manifest digest, upstream baseline, host lifecycle, or effective endpoint capacity.

A documentation clarification alone does not require a connector version. It still needs the source revision that proves the corrected statement.

Record future entries completely

Each future entry should state:

1. release or explicit unreleased status and UTC review date;
2. full AIP source commit, tree, and clean or reconstructable dirty state;
3. connector, image, manifest, catalogue, release, Hermes, and model-route identities;
4. added, changed, fixed, security-relevant, deprecated, and removed surfaces;
5. caller, operator, storage, endpoint, credential, and provider migrations;
6. rollback and compatibility boundary;
7. exact deterministic, image, fleet, path, and live qualification result, or `not_run`;
8. deprecation introduction, replacement, and removal date only when source or release policy defines them.

Do not backfill release history from filenames, mutable tags, or source presence. Mark unknown history as unknown.

Related documentation

- [AIP release notes](#)
- [Migrate bundled connectors to the fleet](#)
- [Hermes scheduled jobs](#)
- [Hermes configuration](#)
- [Qualify the Hermes Agent connector](#)
- [Connector upstream baselines](#)